HKUST – Department of Computer Science and Engineering
COMP170: Discrete Math Tools for CS – FALL 2008

#	LS

Midterm Examination 2

Sketch Solution Key

Date: Tuesday , Nov 11, 2008 Time: 19:00–20:30 Venues: LTA, LTC

Name: _____	Student ID: _____
Email: _____	Lecture and Tutorial: _____

Instructions

- This is a closed book exam. It consists of 21 pages and 8 questions.
- Please write your name, student ID, email, lecture section and tutorial on this page.
- For each subsequent page, please write your student ID at the top of the page in the space provided.
- Please sign the honor code statement on page 2.
- Answer all the questions within the space provided on the examination paper. You may use the back of the pages for your rough work. The last three pages are scrap paper and may also be used for rough work. Each question is on a separate page. This is for clarity and is not meant to imply that each question requires a full page answer. Many can be answered using only a few lines.
- Only use notation given in class. Do not use notation that you have learnt outside of this class that is nonstandard.
- Calculators may be used for the exam.

Questions	1	2	3	4	5	6	7	8	Total
Points	13	12	12	9	15	12	12	15	100
Score									

Student ID: _____

As part of HKUST's introduction of an honor code, the HKUST Senate has recommended that all students be asked to sign a brief declaration printed on examination answer books that their answers are their own work, and that they are aware of the regulations relating to academic integrity. Following this, please read and sign the declaration below.

I declare that the answers submitted for this examination are my own work.

I understand that sanctions will be imposed, if I am found to have violated the University regulations governing academic integrity.

Student's Name: _____

Student's Signature: _____

Student ID: _____

Definitions and Formulas: This page contains some definitions used in this exam and a list of formulas (theorems) that you may use in the exam (without having to provide a proof). Note that you might not need all of these formulas on this exam.

Definitions

1. $N = \{0, 1, 2, 3, \ldots\}$, the set of non-negative integers.
2. $Z^+ = \{1, 2, 3, \ldots\}$, the set of positive integers.
3. Z is the set of *all* integers.
4. R is the set of *real numbers*.
5. R^+ is the set of positive *real numbers*.

Formulas:

1. $\binom{n}{i} = \frac{n!}{i!\,(n-i)!}$
2. If $0 < i < n$ then $\binom{n}{i} = \binom{n-1}{i-1} + \binom{n-1}{i}$
3. $\neg(p \wedge q)$ is equivalent to $\neg p \vee \neg q$
4. $\neg(p \vee q)$ is equivalent to $\neg p \wedge \neg q$
5. $p \Rightarrow q$ is equivalent to $\neg p \vee q$
6. $\neg \forall x \in U\,(p(x))$ is equivalent to $\exists x \in U\,(\neg p(x))$
7. $\sum_{i=1}^{n-1} i = n(n-1)/2$
8. $\sum_{i=1}^{n-1} i^2 = \frac{2n^3-3n^2+n}{6}$
9. If $r \neq 1$ then $\sum_{i=0}^{n-1} r^i = \frac{1-r^n}{1-r}$
10. If $r \neq 1$ then $\sum_{i=0}^{n} ir^i = \frac{nr^{n+2}-(n+1)r^{n+1}+r}{(1-r)^2}$

Student ID: _____

Problem 1: [13 pts] Bob is constructing an RSA key-pair. He first chooses $p = 11$, $q = 19$ and sets $n = 11 \cdot 19 = 209$. He then constructs his public key e and private key d and publishes the (n, e) pair.

(a) Bob's *private* key is $d = 7$. What is the value of his public key e?. Show how you derived your answer.

(b) Alice wants to send Bob a message M, $0 < M < n$. She calculates $X = M^e \bmod n$ to send Bob and finds that $X = 15$. What is the value of the original message M? Explain how you derived your answer.

Solution: **(a)** By the definition of the RSA algorithm $d \cdot e \bmod T = 1$ where $T = (p-1)(q-1) = 10 \cdot 18 = 180$. Using, e.g., the extended GCD algorithm, we find that the multiplicative inverse of 7 mod T is $e = 103$.

(b)

$$M = X^d \bmod n = 15^7 \bmod 209 = 203.$$

(The last equality can be derived any of multiple ways)

Student ID: _____

Problem 2: [12 pts]

Answer the following questions. For parts (a) and (b), do not forget to justify your answers. For part (c), do not forget to show your calculatuons.

(a) Is $(15^{60} \bmod 61) = (15^{62} \bmod 63)$?

(b) Is $(100^{440} \bmod 89) = (100^{1320} \bmod 89)$?

(c) Evaluate $3^{1052} \bmod 60$.

Solution: **(a)** No.
61 is a prime number so, by Fermat's little theorem, $15^{60} \bmod 61 = 1$..
On the other hand, since $3|15$, we also have $3|15^{62}$. Since $3|63$, this means that $3|15^{62} \bmod 63$ so $15^{62} \bmod 63 \neq 1$.

(b) Yes.
89 is prime so, by Fermat's little theorem, $100^{88} \bmod 89 = 1$. Since both 440 and 1320 are divisible by 88 we have

$$\left(100^{440} \bmod 89\right) = 1 = \left(100^{1320} \bmod 89\right).$$

(c) This can be solved by repeated squaring. Set $I_i = 3^{2^i} \bmod 60$. Then

$$\begin{aligned} I_0 &= 3 \\ I_1 &= I^0 \cdot I_0 \bmod 60 = 9 \\ I_2 &= I^1 \cdot I_1 \bmod 60 = 21 \end{aligned}$$

Now notice that $21 \cdot 21 \bmod 60 = 21$ so, for all $i \geq 2$, $I_i = 21$. Since

$$3^{1052} = 3^{1024} \cdot 3^{128}$$

we find

$$(3^{1052} \bmod 60) = (I_7 \cdot I_{10} \bmod 60) = (21^2 \bmod 60) = 21.$$

Student ID: _____

Problem 3: [12 pts] For each of the following pairs of logical statements, either

- Prove that the two statements are logically equivalent, or
- Give a counterexample to show that the statements are not logically equivalent.

Your proof for (a) *may not* use truth tables while your proofs for (b) and (c) may use truth tables, if you find that they help.

A counterexample for (a) would be a truth setting of the variables. A counterexample for (b) or (c) would be some universes U and V and statements $p(x)$ and $q(y)$.

(a) (i) $(p \wedge q) \vee (\neg p \wedge \neg q)$

(ii) $(p \Rightarrow q) \wedge (q \Rightarrow p)$

(b) (i) $\Big(\forall x \in U\ p(x)\Big) \ \Rightarrow\ \Big(\forall x \in U\ q(x)\Big)$

(ii) $\forall x \in U\ \Big(p(x) \ \Rightarrow\ q(x)\Big)$

(c) (i) $\Big(\forall x \in U\ p(x)\Big) \Rightarrow \Big(\exists y \in V\ q(y)\Big)$

(ii) $\exists x \in U\ \exists y \in V\ (p(x) \Rightarrow q(y))$

Solution: **(a)** Logically equivalent.
Using the fact that $(p \to q) \equiv (\neg p \vee q)$ and the distributive laws gives,

$$\begin{aligned}(p \Rightarrow q) \wedge (q \Rightarrow p) &= (\neg p \vee q) \wedge (\neg q \vee p) \\ &= (\neg p \wedge \neg q) \vee (\neg p \wedge p) \vee (q \wedge \neg q) \vee (p \wedge q) \\ &= (p \wedge q) \vee (\neg p \wedge \neg q)\end{aligned}$$

(b) Not logically equivalent.
Consider the following example.
Let $U = R$, $p(x)$ be $x \geq 0$, and $q(x)$ be $-x \geq x$.
$\Big(\forall x \in R\ (x \geq 0)\Big) \ \Rightarrow\ \Big(\forall x \in R\ (-x \geq x)\Big)$
is true because $\Big(\forall x \in R\ (x \geq 0)\Big)$ is false.

On the other hand, $\forall x \in R\ \Big((x \geq 0) \ \Rightarrow\ (-x \geq x)\Big)$ is false.

(c) Logically equivalent. Here is the proof in terms of truth values:

$p(x)$	$q(y)$	$\Big(\forall x\ p(x)\Big) \Rightarrow \Big(\exists y q(y)\Big)$	$\exists x\ \exists y\ (p(x) \Rightarrow q(y))$
always true	always false	false	false
always true	not always false	true	true
not always true	always false	true	true
not always true	not always false	true	true

Alternatively, we can also prove the equivalence using logic laws:

$$\begin{aligned}
\Big(\forall x \in U\ p(x)\Big) \Rightarrow \Big(\exists y \in V\ q(y)\Big) &= \neg\Big(\forall x \in U\ p(x)\Big) \vee \Big(\exists y \in V\ q(y)\Big) \\
&= \Big(\exists x \in U\ \neg p(x)\Big) \vee \Big(\exists y \in V\ q(y)\Big) \\
&= \exists x \in U\ \exists y \in V\ (\neg p(x) \vee q(y)) \\
&= \exists x \in U\ \exists y \in V\ (p(x) \Rightarrow q(y))
\end{aligned}$$

Student ID: _____

Problem 4: [9 pts]

For each of the three statements below, state whether they are True or False. Justify your answer.

(a): $\forall x \in N \;\; \exists y \in R \;\; \Big(y = 2x + 1\Big)$

(b): $\exists y \in R \;\; \forall x \in N \;\; \Big(y = 2x + 1\Big)$

(c): $\exists p \in Z^+ \;\; \Big(\forall x \in Z^+ \;\; \Big[(x < p) \Rightarrow (\exists q \in Z \;\; (x^{p-1} = qp + 1))\Big]\Big)$

Solution:

(a) True. For any $x \in N$, $2x + 1 \in R$

(b) False. For any $y < 0$, $y = 2x + 1$ cannot be true for any $x \in N$. For any $y \geq 0$, $y = 2x + 1$ is not true for $x = y/2$.

(c) True. According to Fermat's little theorem, the statement is true if we choose p to be a prime number.

Student ID: _____

Problem 5: [15 pts] Prove the following statement by contraposition:

> If x and y are two integers such that $0 < x \leq y < 34$ and $x \neq y$, then
>
> $\Big[(x \bmod 5) \neq (y \bmod 5)\Big] \vee \Big[(x \bmod 7) \neq (y \bmod 7)\Big]$.

You may not use the Chinese remainder theorem.

Solution: Let p and q denote the following two sentences:

$$\begin{array}{rcl} p & : & x \text{ and } y \text{ are two integers such that } 0 < x \leq y < 34 \text{ and } x \neq y \\ q & : & \Big[(x \bmod 5) \neq (y \bmod 5)\Big] \vee \Big[(x \bmod 7) \neq (y \bmod 7)\Big] \end{array}$$

The result that we need to prove can be expressed as the conditional statement $p \Rightarrow q$. A contrapositive proof corresponds to proving that $\neg q \Rightarrow \neg p$. We first assume that q is false, i.e.,

$$(x \bmod 5) = (y \bmod 5) \quad \text{and} \quad (x \bmod 7) = (y \bmod 7)$$

This implies $5|(x-y)$ and $7|(x-y)$. Because 5 and 7 are relatively prime, $35|(x-y)$, so $x = y + 35q$ for some integers, q.

There are three cases to consider:

(i) If $q = 0$, then $x = y$ and p is false.

(ii) If $q < 0$, then $y \geq x + 35$ and p is false.

(iii) If $q > 0$, then $x \geq y + 35$ and p is false.

For all three cases, p is false. Thus we have $\neg q \Rightarrow \neg p$.

By the contrapositive rule of inference, we can conclude that $p \Rightarrow q$.

Student ID: _____

Problem 6: [12 pts] Consider the recurrence relation defined by

$$T(n) = \begin{cases} 1 & \text{if } n = 0 \\ 4T(n-1) + 3^n & \text{if } n > 0 \end{cases}$$

Give a closed form solution for $T(n)$.

You must *show your derivation*. That is, you need to show how you derived your solution. This can either be from scratch or by quoting a theorem that we derived in class. It is not necessary, though, to prove the correctness of your solution.

Your solution should *not* contain the summation sign (Σ) or "$\cdots$". As an example, you should not write something like "$\sum_{i=0}^{n-1} 2^i$" or "$1+2+\cdots 2^{n-1}$" in your solution. Instead, you should write "$2^n - 1$".

Solution: By iterating the recurrence we derive that

$$T(n) = 4^n + \sum_{i=1}^{n} 4^{n-i} f(i). \tag{1}$$

Plugging $f(i) = 3^i$ into (1) gives

$$\begin{aligned} T(n) &= 4^n + \sum_{i=1}^{n} 4^{n-i} 3^n \\ &= 4^n + 4^n \sum_{i=1}^{n} \left(\frac{3}{4}\right)^i \\ &= 4^n + 4^n \frac{3}{4} \sum_{i=0}^{n-1} \left(\frac{3}{4}\right)^i \\ &= 4^n + 3 \cdot 4^n \left(1 - \left(\frac{3}{4}\right)^n\right) \\ &= 4^{n+1} - 3^{n+1}. \end{aligned}$$

Student ID: _____

Problem 7: [12 pts] Consider the recurrence relation defined by

$$T(n) = \begin{cases} 5 & \text{if } n = 1 \\ 9T\left(\frac{n}{3}\right) + 2n & \text{if } n > 1. \end{cases}$$

For the purposes of this problem, you may assume that n is a power of 3.

(a) Give a closed form solution to $T(n)$.
As in the previous question, your solution may not ontain the summation sign (Σ) or "$\cdots$".
It is not necessary to show the derivation of your solution.

(b) Prove the correctness of your solution using induction.

Solution: **(a)**

$$T(n) = 6n^2 - n.$$

(b) **Base case:**
Let $n = 1$. $T(1) = 5 = 6 \cdot 1^1 - 1$. So the base case is true.
Inductive case:
Suppose the statement is true for 3^{i-1}, with $i > 0$. Let $n = 3^i$. By definition,

$$\begin{aligned} T(n) &= 9\left(6\left(\frac{n}{3}\right)^2 - \frac{n}{3}\right) + 2n \\ &= 6n^2 - 3n + 2n \\ &= = 6n^2 - n, \end{aligned}$$

so the statement is true for $n = 3^i$. From weak principle of mathematical induction, we conclude that the statement is true for $n = 3^i$, $\forall i \geq 0$.

Student ID: _____

Problem 8: [15 pts] Prove by induction that if $T(n)$ is defined by

$$T(n) = \begin{cases} 1 & \text{if } n = 0 \\ \sqrt{1 + 3\sum_{i=0}^{n-1} (T(i))^2} & \text{if } n \geq 1. \end{cases}$$

then $\forall n \geq 0$, $T(n) = 2^n$.

Solution: **Base case:** Let $n = 0$. $T(0) = 2^0 = 1$. So the base case is true.
Inductive case: Let $n > 0$. The statement is true from 1 to $n - 1$.
i.e.,

$$T(1) = 2^1, \quad T(1) = 2^2, \quad \ldots \quad T(n-1) = 2^{n-1}$$

$$\begin{aligned} T(n) &= \sqrt{1 + 3\sum_{i=0}^{n-1} (T(i))^2} \\ &= \sqrt{1 + 3\sum_{i=0}^{n-1} (2^i)^2} \\ &= \sqrt{1 + 3\sum_{i=0}^{n-1} 2^{2i}} \\ &= \sqrt{1 + 3\sum_{i=0}^{n-1} 4^i} \\ &= \sqrt{1 + 3(\frac{4^n - 1}{4 - 1})} \\ &= \sqrt{1 + 4^n - 1} \\ &= \sqrt{2^{2n}} \\ &= 2^n \end{aligned}$$

Based on the strong principle of mathematical induction, we conclude that the statement is true for all integers $\forall n \geq 0$.